Math 2070 Week 4

Lagrange's Theorem, Generators, Group Homomorphisms

4.1 Lagrange's Theorem

Theorem 4.1 (Lagrange's Theorem)**.** *Let G be a finite group. Let H be subgroup of G, then $|H|$ divides $|G|$. More precisely, $|G| = [G : H] \cdot |H|$.*

Proof. We already know that the left cosets of H partition G. That is:

$$G = a_1 H \sqcup a_2 H \sqcup \ldots \sqcup a_{[G:H]} H,$$

where $a_i H \cap a_j H = \emptyset$ if $i \neq j$. Hence, $|G| = \sum_{i=1}^{[G:H]} |a_i H|$.

The theorem follows if we show that the size of each left coset of H is equal to $|H|$.

For each left coset S of H, pick an element $a \in S$, and define a map $\psi : H \longrightarrow S$ as follows:

$$\psi(h) = ah.$$

We want to show that ψ is bijective.

For any $s \in S$, by definition of a left coset (as an equivalence class) we have $s = ah$ for some $h \in H$. Hence, ψ is surjective.

If $\psi(h') = ah' = ah = \psi(h)$ for some $h', h \in H$, then $h' = a^{-1}ah' = a^{-1}ah = h$. Hence, ψ is one-to-one.

So we have a bijection between two finite sets. Hence, $|S| = |H|$. $\square$

Corollary 4.2. *Let G be a finite group. The order of every element of G divides the order of G.*

Since G is finite, any element of $g \in G$ has finite order $\operatorname{ord} g$. Since the order of the subgroup:

$$H = \langle g \rangle = \{e, g, g^2, \ldots, g^{(\operatorname{ord} g)-1}\}$$

is equal to $\operatorname{ord} g$, it follows from Lagrange's Theorem that $\operatorname{ord} g = |H|$ divides $|G|$.

Corollary 4.3. *If the order of a group G is prime, then G is a cyclic group.*
Proof shown in class

Corollary 4.4. *If a group G is finite, then for all $g \in G$ we have:*

$$g^{|G|} = e.$$

Proof shown in class

Corollary 4.5. *Let G be a finite group. Then a nonempty subset H of G is a subgroup of G if and only if it is closed under the group operation of G (i.e. $ab \in H$ for all $a, b \in H$).*

Proof. It is easy to see that if H is a subgroup, then it is closed under the group operation. The other direction is left as an **Exercise**. □

Example 4.6. *Let n be an integer greater than 1. The group A_n of even permutations on a set of n elements (see Example 3.4) has order $\frac{n!}{2}$.*

Proof. View A_n as a subgroup of S_n, which has order $n!$.
Exercise: Show that $S_n = A_n \sqcup (12)A_n$.
Hence, we have $[S_n : A_n] = 2$.
It now follows from Lagrange's Theorem that:

$$|A_n| = \frac{|S_n|}{[S_n : A_n]} = \frac{n!}{2}.$$

□

4.1.1 WeBWorK

1. **WeBWorK**
2. **WeBWorK**
3. **WeBWorK**
4. **WeBWorK**

4.2 Generators

Let G be a group, X a nonempty subset of G. The subset of G consisting of elements of the form:

$$g_1^{m_1} g_2^{m_2} \cdots g_n^{m_n}, \quad \text{where} \quad n \in \mathbb{N}, g_i \in X, m_i \in \mathbb{Z},$$

is a subgroup of G. We say that it is the subgroup of G **generated** by X. If $X = \{x_1, x_2, \ldots, x_l\}$, $l \in \mathbb{N}$. We often write:

$$\langle x_1, x_2, \ldots, x_l \rangle$$

to denote the subgroup generated by X.

Example 4.7. *In D_n, $\{r_0, r_1, \ldots, r_{n-1}\} = \langle r_1 \rangle$.*

If there exists a finite number of elements $x_1, x_2, \ldots, x_l \in G$ such that $G = \langle x_1, x_2, \ldots, x_l \rangle$, we say that G is **finitely generated**.

For example, every cyclic group is finitely generated, for it is generated by one element.

Every finite group is finitely generated, since we may take the finite generating set X to be G itself.

Example 4.8. *Consider $G = D_3$, and its subgroup $H = \{r_0, r_1, r_2\}$ consisting of its rotations. (We use the convention that r_k is the anticlockwise rotation by an angle of $2\pi k/3$).*

By Lagrange's Theorem, the index of H in G is $[G : H] = |G| \,/\, |H| = 2$. This implies that $G = H \sqcup gH$ for some $g \in G$. Since $gH = H$ if $g \in H$, we may conclude that $g \notin H$. So, g is a reflection.

Conversely, for any reflection $s \in D_3$, the left coset sH is disjoint from H. We have therefore $G = H \sqcup s_1 H = H \sqcup s_2 H = H \sqcup s_3 H$, which implies that $s_1 H = s_2 H = s_3 H$.

In particular, for a fixed $s = s_i$, any element in G is either a rotation or equal to sr_i for some rotation r_i. Since H is a cyclic group, generated by the rotation r_1, we have $D_3 = \langle r_1, s \rangle$, where s is any reflection in D_3.

4.3 Group Homomorphisms

Definition 4.9. *Let $G = (G, *)$, $G' = (G', *')$ be groups. A* **group homomorphism** *ϕ from G to G' is a map $\phi : G \longrightarrow G'$ which satisfies:*

$$\phi(a * b) = \phi(a) *' \phi(b),$$

for all $a, b \in G$.

Claim 4.10. *If $\phi : G \longrightarrow G'$ is a group homomorphism, then:*

1. $\phi(e_G) = e_{G'}$.
2. $\phi(g^{-1}) = \phi(g)^{-1}$, *for all* $g \in G$.
3. $\phi(g^n) = \phi(g)^n$, *for all* $g \in G$, $n \in \mathbb{Z}$.

Proof. We prove the first claim, and leave the rest as an exercise. Since e_G is the identity element of G, we have $e_G * e_G = e_G$. On the other hand, since ϕ is a group homomorphism, we have:

$$\phi(e_G) = \phi(e_G * e_G) = \phi(e_G) *' \phi(e_G).$$

Since G' is a group, $\phi(e_G)^{-1}$ exists in G', hence:

$$\phi(e_G)^{-1} *' \phi(e_G) = \phi(e_G)^{-1} *' (\phi(e_G) *' \phi(e_G))$$

The left-hand side is equal to $e_{G'}$, while by the associativity of $*'$ the right-hand side is equal to $\phi(e_G)$. $\square$

Let $\phi : G \longrightarrow G'$ be a homomorphism of groups. The image of ϕ is defined as:

$$\operatorname{im} \phi := \phi(G) := \{\phi(g) : g \in G\} \subseteq G'$$

The kernel of ϕ is defined as:

$$\ker \phi = \{g \in G : \phi(g) = e_{G'}\} \subseteq G.$$

Claim 4.11. *The image of ϕ is a subgroup of G'. The kernel of ϕ is a subgroup of G.*

Claim 4.12. *A group homomorphism $\phi : G \longrightarrow G'$ is one-to-one if and only if* $\ker \phi = \{e_G\}$.

Proof shown in class

Example 4.13 (Examples of Group Homomorphisms).

- $\phi : S_n \longrightarrow (\{\pm 1\}, \cdot)$,

$$\phi(\sigma) = \begin{cases} 1, & \sigma \textit{ is an even permutation.} \\ -1, & \sigma \textit{ is an odd permutation.} \end{cases}$$

  $\ker \phi = A_n$.

- $\det : \mathrm{GL}(n, \mathbb{R}) \longrightarrow (\mathbb{R}^\times, \cdot)$

  $\ker \det = \mathrm{SL}(n, \mathbb{R})$.

- *Let G be the (additive) group of all real-valued continuous functions on $[0,1]$.*

$$\phi : G \longrightarrow (\mathbb{R}, +)$$
$$\phi(f) = \int_0^1 f(x)\,dx.$$

- $\phi : (\mathbb{R}, +) \longrightarrow (\mathbb{R}^\times, \cdot)$.

$$\phi(x) = e^x.$$

Definition 4.14. *Let G, G' be groups. A map $\phi : G \longrightarrow G'$ is a group* **isomorphism** *if it is a bijective group homomorphism.*

Note that if a homomorphism ϕ is bijective, then $\phi^{-1} : G' \longrightarrow G$ is also a homomorphism, and consequently, ϕ^{-1} is an isomorphism. If there exists an isomorphism between two groups G and G', we say that the groups G and G' are **isomorphic**.

Example 4.15. *Recall Definition 3.1 and Exercise 3.2.*

Let $n > 2$. Let $H = \{r_0, r_1, r_2, \dots, r_{n-1}\}$ be the subgroup of D_n consisting of all rotations, where r_1 denotes the anticlockwise rotation by the angle $2\pi/n$, and $r_k = r_1^k$. Then, H is isomorphic to $\mathbb{Z}_n = (\mathbb{Z}_n, +_{\mathbb{Z}_n})$.

Proof. Define $\phi : H \longrightarrow \mathbb{Z}_n$ as follows:

$$\phi(r_k) = k, \quad k \in \{0, 1, 2, \dots, n-1\}.$$

For any $k \in \mathbb{Z}$, let $\overline{k} \in \{0, 1, 2, \dots, n-1\}$ denote the remainder of the division of k by n. By the Division Theorem for Integers, we have:

$$k = nq + \overline{k}$$

for some integer $q \in \mathbb{Z}$.

It now follows from $\operatorname{ord} r_1 = n$ that, for all $r_i, r_j \in H$, we have:

$$\begin{aligned} r_i r_j &= r_1^i r_1^j = r_1^{i+j} \\ &= r_1^{nq+\overline{i+j}} \\ &= (r_1^n)^q\, r_1^{\overline{i+j}} \\ &= r_{\overline{i+j}}. \end{aligned}$$

Hence,

$$\begin{aligned} \phi(r_i r_j) &= \phi(r_{\overline{i+j}}) \\ &= \overline{i+j} \\ &= i +_{\mathbb{Z}_n} j \\ &= \phi(r_i) +_{\mathbb{Z}_n} \phi(r_j). \end{aligned}$$

This shows that ϕ is a homomorphism. It is clear that ϕ is surjective, which then implies that ϕ is one-to-one, for the two groups have the same size. Hence, ϕ is a bijective homomorphism, i.e. an isomorphism. $\square$